Amendments to the Specification

Please replace the paragraph at page 9, lines 9-11 with the following replacement paragraph:

(1) external networks including a public switched telephone network (PSTN) ~~170~~160, ~~an~~ signaling system 7 (SS7) network 170, an Internet 180, and/or a wireless network 144;

Please replace the paragraph at page 13, lines 3 – 25 with the following replacement paragraph:

In exemplary embodiments, the dynamic host control protocol server 131 and domain name service server 214 may operate to dynamically assign IP addresses devices in the customer premise equipment 102. Where a dynamic IP assignment scheme is used, the customer premises equipment may be provided with one or a plurality of dynamic IP assignment when activated initially, and/or at the initiation of each active secession. Where an IP address is assigned when the device is initially activated, it may be desirable to assign a single IP address to a single broadband residential gateway and assign a port address to devices connected to the broadband residential gateway 300. In other embodiments, an individual IP address may be assigned to each device coupled to the broadband residential gateway 300. For example, the broadband residential gateway may include and/or be coupled to one or more cable modems, IP phones, plain old telephone system phones, computers, wireless devices, CATV converters, video phones, and/or other devices which each may be assigned a unique static and/or dynamic IP address and/or a port of a one of these IP addresses. The particular protocol for allocating IP addresses and/or ports may be specified using protocols defined in the dynamic host control protocol server 214. In exemplary embodiments, the dynamic host control protocol server 131 and DN server 214 may be configured to assign available IP addresses from address pools based, for example, on the identity or type of requesting device, the amount of use expected for the requesting device, and/or predefined assignment protocols defined in the dynamic host control protocol server 131 and DN

server 214. In centralized embodiments, it may be desirable to configure the call manager (CM) 218 to provide sufficient information such that the domain name service server 214 can distinguish between static IP devices, dynamic IP devices, registered devices, unregistered devices, and registered devices that have been assigned to a particular class of service e.g., data vs. telephony, un-provisioned, vs. provisioned, etc.

C2

Please replace the paragraph at page 13, lines 26 – 30 with the following replacement paragraph:

The trivial file transfer protocol (TFTP) server ~~214~~ 132 may be configured to transfer certain information to/from one or more broadband residential gateways 300. In exemplary embodiments, the trivial file transfer protocol server 132 provides Data Over Cable Service Interface Specifications (DOCSIS) configuration information containing QoS parameters and other information required for the broadband residential gateway 300 to operate optimally.

Please replace the paragraph at page 26, line 26 – page 28, line 10 with the following replacement paragraph:

C3

Where the elements of the broadband residential gateway 300 are interconnected, the interconnection may be provided by one or more data buses, for example, a high speed bus (HSB) 360, processor bus 380, and/or other interconnection system. The high speed bus 360~~, 380~~ may be configured to provide a flexible conduit for transferring information between the internal hardware, processors and ports. In exemplary embodiments of the broadband residential gateway 300, the high speed bus 360 may include one or more of the following functional units a) a universal remote control receiver module 365 for receiving wireless (e.g., infrared, and/or RF) signals (e.g., keyboard signals and/or remote control signals) for control of the broadband residential gateway 300 and/or any connected devices, b) a display, display driver, touch screen logic module for driving one or more local and/or remote displays for interfacing with the broadband residential gateway 300 and/or one or more connected devices, c) one or more TV port modules 336 for interconnecting televisions, set-top devices, and/or other audiovisual devices to the broadband residential gateway 300, d) one or more data port

modules 334 for connecting/interconnecting data enabled devices (e.g., personal computers, palm top devices, etc.), e) one or more telephony port modules 332 for interconnecting one or more analog and/or digital telephones, f) one or more peripheral port modules 342 for interconnecting one or more peripheral devices such as disk drives, data storage devices, video cassette recorders, DVD devices, audio devices, video devices (e.g., camcorders, digital cameras, digital video recorders, stereos, etc.), g) one or more external/internal intercom modules 344 for interconnecting remote intercom and/or security monitoring devices, h) one or more wireless interface modules 345 for interconnecting with various wireless extension devices such as wireless TVs, cordless and/or wireless telephones, wireless LANs, etc., i) one or more voice recognition/voice synthesis modules 355 for generating voice announcements, voice messages, and voice prompts and for recognizing voice generated commands and data, j) set-top box module 350 for performing the functions associated with a set-top box locally and/or for communicating with one or more remotely coupled set-top boxes, k) memory 322 (e.g., DRAM, RAM, flash, and/or other memory) for storing information and operating data within the broadband residential gateway 300, l) transceiver 302 for communicating with one or more external broadband networks m) operating program store 330 (e.g., ROM, flash, etc.) for storing at least portions of the operating programs for the broadband residential gateway 300 and/or interconnected devices, n) security processor, smart card and/or credit card interface module 340 for providing secure processing functions and/or credit card/smart card transaction functions, and/or o) distributed processing controller 306 which may be a microprocessor and/or one or more interconnected distributed processing modules for controlling the broadband residential gateway 300. Where the distributed processing controller 306 includes one or more distributed processing modules, the modules may include a telephony processing module (P1) 308, data processing module (P2~~3~~) 310, video processing module (P3) 312, auxiliary processing module (P4) 314, IP processing module (P5) 316, and/or an operations administration maintenance and provisioning processing module (P6) 318 interconnected through one or more busses such as processor bus 380. The processor bus 380 and/or high speed bus 360 may include any suitable interconnect bus including intelligent bus configurations incorporating smart buffer logic (not shown in Fig. 3) to facilitate data transfer between

C3

interconnected processors and/or modules. The various modules and/or processing components of the broadband residential gateway 300 may be powered by , for example, a power supply unit (not shown). Each of the individual modules of the broadband residential gateway will now be described in more detail.

Please replace the paragraph at page 35, line 13 – page 36, line 2 with the following replacement paragraph:

C4

In the embodiment shown in Fig. 4, the high speed network 120n includes the ultra high-speed routers (UHR) 121 configured in a ring configuration. Although this embodiment shows the use of the IP network database (IND) 122, other configurations are also suitable. Where an IP network database 122 is utilized, it may be desirable to incorporate one or more data sets such as: a IP local number portability database (IP LNP) ~~122a~~ which may be utilized for transferring local DN among service providers when a user changes their service provider; an IP caller name database (IP CNAME) ~~122b~~ which may be utilized to provide a database of names relating to IP addresses and/or domain names; an IP line information database (IP LIDB) ~~122c~~ which may provide alternative billing and allow flexibility in determining who pays for a call; and an IP 1-800 Database (IP 8YY) ~~122d~~ which may provide a database of 1-800 numbers relating to the IP network 120a. Alternatively, the IP local number portability database may be located at another location, such as at an IP central station (IP Central) 200. Where desired, a local service management system (LSMS) 150 may be arranged to provide management of the IP local number portability database. Where a local service management system 150 is utilized, a plurality of local service order administration (LSOA) units 152 may be coupled to the local service management system by, for example, a number portability administration center (NPAC) 151. In this manner, directory numbers may be transported among different service providers. In such a case, a NPAC 151 is generally coupled to the LSMS 150 and uses the LSMS 150 to synchronize the numbering databases and to coordinate the porting process.

Please replace the paragraph at page 37, lines 11 – 26 with the following replacement paragraph:

C15

In one exemplary application of the voice over IP operations, the broadband residential gateway 300 digitizes the analog telephony signal using, for example, G.711 μ law coding (64 Kbps Pulse Code Modulation). The digital samples may then be packetized in, for example, the broadband residential gateway 300 into IP packets. The broadband residential gateway 300 may be configured to encapsulate the IP packets into, for example, DOCSIS (Data Over Cable Service Interface Specifications) frames for transmission back to the head-end hub (HEH) 115 over the hybrid fiber-coaxial plant 112. The hybrid fiber-coaxial plant 112 may then be configured to transport signals for both upstream (to head-end hub ~~202~~ 115) and downstream (to the broadband residential gateway 300 and customer premise equipment 102) directions. Although the DOCSIS protocol is utilized in this example, any future protocol may also be used for the digitizing and packeting of data. Where the protocol changes, it may be desirable to download new operating code from, for example, IP central station 200 to the individual broadband residential gateways 300, to update the communication protocols dynamically. When new protocols are adopted, the IP central station may utilize, for example, the system management server 216 to download new protocol data into, for example, the protocol manager in the call manager 218 and the program store 330 in the broadband residential gateway 300.

Please replace the ABSTRACT with the following replacement ABSTRACT:

NE.

Communication information transmitted in the broadband communication system may be in a packet format and secured using encryption techniques, for example encryption software, including a means for providing an initial security key and updated security keys to the various pieces of communication equipment located throughout the broadband communication system. When communication equipment, for example a gateway, is first registered with, for example, an IP central station, the IP central station assigns an initial encryption key to the gateway that is assigned and retained by a server, for example a call manager ~~(CM)~~ server, and the gateway (e.g., broadband residential

gateway ~~(BRG)~~). This initial encryption key may be used to establish a secure two way communication between two pieces of communication equipment as an originating point communication equipment ~~(OPCE)~~ and a terminating point communication equipment. ~~(TPCE), for example, the BRG (OPCE) and the CM (TPCE), the BRG (OPCE), BRG1, and another BRG (TPCE), BRG2, or the BRG and a gateway for interfacing with another communication system (e.g. VG). Whenever a user first activates a secure communication feature before or during a communication session, the origination point communication equipment (e.g., BRG1) will not send the terminating point communication equipment (e.g., BRG2) a packet including a private key which may be the BRG's initial encryption key. Subsequently the two pieces of communication equipment will encrypt and decrypt communication packets to one another using the private key. The secured encrypted packets may be part of one or more legs in, for example, a conference call, a teleconference, or a multimedia session. The encryption key may be repeatedly updated and changed at various time intervals. The repeated updates may be at periodic (e.g., daily) or at random time intervals. Updates of the encryption key may occur when the secure call feature is active or inactive. For additional security the system may assign a unique randomly generated encryption key to each packet during the communication session and provide each new key to the communication equipment (e.g., BRG) in each prior information packet transmission. A secure call feature may be activated and deactivated by the user at anytime before or during (i.e., real time activation) an existing communication session. The secure call feature may be used to secure one type of media using encryption while not securing other types of media in a multimedia communication session. Alternatively, different media types, for example audio, text, and multimedia audio and video, may be secured at different levels of security using for example different encryption types or algorithms (e.g., DES, PGP, RSA, etc.). A server, for example a call manger (CM), may coordinate a secure communication between two pieces of communication equipment by translating between two different encryption algorithms in two separate legs of a communication session (e.g., a telephone call). Alternatively, the server may send encryption algorithms to a piece of communication equipment so that the various pieces of communication equipment are using the same algorithm. Control of the secure communication may be~~

~~transferred from, for example an originating gateway to a terminating gateway. In this case the encryption of a secure communication session may begin by using the originating gateway's key but then start using the terminating gateway's key. The on net communications, for example telephone calls, within the broadband communication system may be encrypted but the on net to off net communications for example telephone calls including PSTN portion, may be partially encrypted. Once the communication enters for example the PSTN, it has only that security provided by the traditional wireline PSTN.~~